UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMANDA MARBLE AND KELSEY REIMER, individually and on behalf of all others similarly situated,
 	
    Plaintiffs,
 	
v.
 	
HALO INNOVATIONS, INC.,
 	
    Defendant.
	Case No. 1:23-cv-11048

[PROExtranet OSED] ORDER GRANTING AGREED MOTION FOR ENTRY OF
PROTOCOL REGARDING DISCOVERY OF ELECTRONICALLY
STORED INFORMATION

Plaintiffs Amanda Marble and Kelsey Reimer ("Plaintiffs") and Defendant Halo, Innovations, Inc. ("HALO") (collectively, "Parties") stipulate and agree, by and through their respective counsel, subject to the approval of the Court, that the following Agreed Order Regarding the Discovery of Electronically Stored Information (the "Stipulated ESI Protocol" or the "Protocol") be entered by this Court, and shall govern the subject action:

1.   PURPOSE

This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure, this Court's Local Rules, and any other applicable orders and rules.

2.   COOPERATION

The Parties are expected to use reasonable, good faith and proportional efforts to preserve, identify, and produce relevant and discoverable information consistent with Fed. R. Civ. P. 26(b)(1). "Parties may obtain discovery regarding any nonprivileged matter that is

relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable." Fed. R. Civ. P. 26(b)(1).

3.   PROPORTIONALITY

A.   The Parties will consider the proportionality standard set forth in Fed. R. Civ. P. 26(b)(2)(C) in formulating their discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as practicable.

B.   The Parties will consider the option of prioritizing certain discovery where appropriate. In order to reduce the costs and burdens of discovery, the Parties have agreed that this ESI Protocol shall incorporate a non-waiver agreement pursuant to Federal Rule of Evidence 502(d), which states in full: "(d) Controlling Effect of a Court Order. A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding." Fed. R. Evid. 502(d).

4.   PRESERVATION OF ESI

A.   The Parties acknowledge that they have an obligation to take reasonable and proportional steps to preserve discoverable information in the Party's possession, custody or control.

B.   The Parties agree that a significant quantity of relevant information can be yielded

from reasonably accessible sources and, as necessary and appropriate, supplemented with deposition discovery. The possibility of additional relevant information existing that is not reasonably accessible is substantially outweighed by the burden and cost of preservation, collection, review and production of ESI from such sources. The Parties agree that the following ESI is not reasonably accessible:

i. Data maintained or duplicated in any electronic backup system for the purpose of system recovery or information restoration, including but not limited to, system recovery backup tapes or other media, continuity of operations systems, and data or system mirrors or shadows, if such data are routinely purged, overwritten or otherwise made not reasonably accessible in accordance with an established routine system maintenance policy.

ii. Unallocated, slack space, deleted data, file fragments, or other data not accessible by use of computer forensics;

iii. Random access memory (RAM), temporary files, or other ephemeral data that is difficult to preserve;

iv. Data relating to online access, such as temporary Internet files, browser history, file or memory caches and cookies;

v. Data in metadata fields that are frequently updated automatically as part of the usual operation of a software application, operating system or network (e.g., data last opened) provided, however, that such metadata as it exists at the time of preservation shall be retained, produced, and not altered by the production process unless it is separately preserved and

produced with the relevant document;

vi. Telephone or VOIP voice messages that are not regularly stored or saved, unless any such messages were otherwise stored or saved;

vii. Instant messages such as messages sent on Lync Online, Microsoft Communicator, Google Chat, or any other instant message platform if not maintained in the ordinary course of business.

viii. Data stored on cell phones or mobile devices, excluding tablets, that is more reasonably accessible elsewhere, provided that the alternative location is identified, the producing Party shall produce such data from reasonably accessible sources along with documentation of the specific device on which it is also located, and the producing Party shall do so without any additional request for production from the receiving Party. Further, all such devices that were identified and that contain data that was not preserved shall be identified;

ix. Call history records maintained on mobile devices, cell phones or Blackberry devices so long as copies of telephone bills that contain such records are made available when responsive;

x. Operating system files, executable files, and log files (including web server, web services, system, network, application log files and associated databases, analysis output caches, and archives of such data), unless such log files may be used to identify putative class members; and

xi. Other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business. If a Party

identifies such a form of ESI during its efforts to identify responsive information, that Party shall promptly meet and confer with the other Parties to discuss the nature of the ESI, its potential relevance to the case, and the burdens of preservation.

C.   Absent a showing of good cause, no Party need restore any form of media upon which backup data is maintained in a Party's normal or allowed processes, including but not limited to backup tapes, disks, SAN, and other forms of media, to comply with its discovery obligations in the present case. For the avoidance of doubt, CDs, DVDs or other media that are used in the ordinary course of business to store original data shall be searched for responsive material.

5.   SOURCES OF ESI

A.   The Parties agree to limit searches of discoverable ESI as follows. Collections of ESI shall be initially limited to up to 10 key custodians per Party. Each Party shall designate its own custodians, and, upon designation, disclose the identities of the custodians to the other Party along with the custodians' title, job description, and length of employment. HALO shall also produce an organizational chart for the years 2021 - 2023, identifying individuals in the design, manufacturing, marketing, and sales teams and how they fit in the corporate hierarchy, if reasonably available. This includes individuals HALO intends to identify as a custodian for the purpose of producing ESI. Should the other Party have a reasonable basis to question the choices of custodians, the Parties agree to meet and confer about the designated custodians. A Party seeking collections from additional custodians shall meet and discuss a reasonable resolution with the other Parties, including outlining the good faith need for the additional collections and whether the request is proportionate to the needs of the case. Should the Parties be unable to

agree on whether there is a good faith need for additional custodians or additional collections, the requesting Party shall seek relief from the court. In the event a Party requests and receives court approval for collections from more than 10 custodians of another Party's ESI, the requesting Party shall reimburse the producing Party for the additional expenses of searching for, collecting, reviewing, and producing any responsive ESI from those additional custodians.

B.   The Parties further agree to be bound by the Stipulated Protective Order during the sharing of ESI. Nothing in this Stipulated ESI Protocol precludes any Party from challenging the admissibility, discoverability, production, relevance, or confidentiality of information produced under this Protocol or otherwise objecting to its production or use at trial.

C.   No Party may seek relief from the Court concerning compliance with the Protocol unless it has conferred with other affected Parties.

D.   If necessary, the Stipulated ESI Protocol may be amended by written modification of all Parties and approval by the court.

6.   ESI DISCOVERY PLAN

A.   The ESI search period shall be January 1, 2021-December 19, 2023 unless the time period is otherwise identified in the discovery requests and pre-dates January 1, 2021. Nothing herein shall restrict a Party from objecting to any discovery requests. The parties will meet and confer regarding what search terms may be applicable to a time period that pre-dates January 1, 2021, and promptly bring any dispute to the Court for resolution.

B.   Each Party will be responsible for reviewing and producing its own documents consistent with Federal Rules of Civil Procedure. To facilitate a cooperative, efficient, and cost effective discovery process, the Parties agree to meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and to filter out ESI that is not

subject to discovery. Documents or categories of documents that are easily identifiable and segregable shall be collected without the use of search terms or other agreed-upon advanced search methodology (e.g., analytics, predictive coding, Computer Assisted Learning ("CAL") or Technology Assisted Review ("TAR")).

C.   The Parties shall meet and confer promptly following entry of this Order to discuss proposals to identify key custodians with potentially-responsive information, non-custodial sources of potentially-responsive information (e.g., relevant databases or other repositories of data or documents), and relevant search terms and limitations.

D.   Each Party may serve its initial written discovery requests in accordance with the joint case management plans and related scheduling orders.

E.   If a Party employs a methodology other than keyword searching to identify responsive documents, it will provide the Requesting Party with the identity of its CAL or TAR tool(s), and will, meet and confer to negotiate the methodology by which such tools will be applied. Agreement on a search methodology does not relieve a party of its obligation to conduct a reasonable search and produce all relevant and responsive documents of which a party is aware, regardless of whether they contain search terms or some other search methodology agreed to by the parties or ordered by the Court.

7.   GENERAL PRODUCTION FORMAT

A.   The Parties will produce ESI in TIFF image format provided that the documents do not become illegible or unusable or in any way alter existing metadata when converted to TIFF image format. Any Party may request production of the native format of any document produced in any non-native format. If a dispute arises as to the reasonableness of the request, the Parties agree to meet and confer in an effort to resolve their differences.

B.   Certain documents that become illegible or unusable when converted to TIFF image format (Microsoft Excel files, other similar spreadsheet application files, Microsoft Project, PowerPoint, and audio and video files), must be produced in native format, unless they contain information that requires redaction.

       i.   Excel (or other spreadsheet formats) will be produced in native format. Native Excel files will be redacted by overwriting the data contained in a particular cell, row, column or tab with the word "REDACTED." These documents will be identified as redacted within the "REDACTED" field in the .DAT. If the producing Party deems it necessary to produce redacted Excel (or other spreadsheet formats) in any format other than Native, the Parties should meet and confer before such a production is made.

       ii.   PowerPoint (or other presentation formats) will be produced in native format. Native PowerPoint presentations that require redactions shall be produced as TIFF images, which shall include speaker notes and "hidden" slides as extracted by the software used to process the documents. Color PowerPoint presentations requiring redactions shall be converted to color images, and black and white PowerPoint presentations requiring redactions shall be converted to black and white TIFF images, provided that proper grayscale printing is enabled to ensure that any dark colored text is not hidden by dark objects/drawings around the text. If the PowerPoint or slide program contains video or audio components, the video or audio will be produced as native files with the appropriate

attachment relationships.

  iii. Word processing documents with redactions will be processed to TIFF format and imaged showing track changes or edits, comments, notes and other similar information.

The Parties reserve their rights to seek additional electronic documents in their native format, including natively redacted spreadsheet documents that preserve the searching, sorting, and filtering characteristics intrinsic to spreadsheet functionality. Electronic documents should be produced in such fashion as to identify the location (i.e., the network file folder, hard drive, back-up tape or other location) where the documents are stored and, where applicable, the natural person in whose possession they were found (or on whose hardware device they reside or are stored).

  C. All production documents will be produced with extracted text and load files including the data fields provided in **Exhibit A**. In those instances where redaction is used, OCR text will be provided in lieu of the extracted text to allow for removal of the redacted text from production. For documents produced in native format, in addition to producing extracted text and the data fields in the table below, the producing Party will provide slip sheets endorsed with the production number and level of confidentiality pursuant to any applicable protective orders in this case.

  D. Non-electronic documents shall be scanned into a static-image format. Copies of file folders and identification of file custodians shall be produced.

  E. For documents that have originated in paper format, the following specifications should be used for their production.

  i. Each unique document must be produced as a separate document. To the

extent there are hard copy emails with attachments those documents must be produced separately with the BEGATT and ENDATT metadata fields populated to connect the family members.

ii.   Each filename must be unique and match the Bates number of the page. The filename should not contain any blank spaces and should be zero padded (for example ABC00000001).

iii.   Media may be delivered via secure FTP or hard drive due to size. Each media volume should have its own unique name and a consistent naming convention (for example ZZZ001 or SMITH001).

iv.   Each delivery should be accompanied by an image cross reference file that contains document breaks.

v.   Each of the metadata and coding fields set forth below that can be extracted shall be produced for each document. The Parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document, with the exception of the following: (a) PRODBEG, (b) PRODEND, (c) BEGATT, (d) ENDATT, (e) CUSTODIAN, (f) ALL CUSTODIAN, (g) NATIVEFILEPATH, (h) TEXTFILEPATH, (i) HASHVALUE; (j) DOCTYPE, (k) CONFIDENTIALITY and (l) PGCOUNT which should be populated by the Party or the Party's vendor. The Parties will make reasonable efforts to ensure that metadata fields automatically extracted from the documents correspond directly to the information that exists in the original documents.

vi.   The standard delimiters for the metadata load file should be: Field Separator, ASCII character 020: " " Quote Character, ASCII character 254 "þ" Multi-Entry Delimiter, ASCII character 059: ";"

vii.   When subjecting physical documents to an OCR process, the settings of the OCR software shall maximize text quality over process speed. Any settings such as "auto-skewing," "auto- rotation," and the like should be turned on when documents are run through the process. In scanning paper documents, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records (i.e., paper documents should be logically unitized). Parent-child relationships (the association between attachments and their parent documents) shall be preserved. In the case of an organized compilation of separate documents -- for example, a binder containing several separate documents behind numbered tabs -- the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the beginning and ending document and attachment fields. Original Document orientation shall be maintained (i.e., portrait to portrait and landscape to landscape). The Parties agree to meet and confer as to any dispute before the issue is submitted to the court."

8.   **IMAGE FORMAT**

A.   Documents that are converted to TIFF image format will be produced in accordance with the following technical specifications:

       i.   Images will be single-page, Group IV TIFF image files at 300 dpi;

       ii.   TIFF file names cannot contain embedded spaces;

       iii.   Bates numbers should be endorsed on the lower right corner of all TIFF images and will be a unique, consistently formatted identifier, i.e. alpha prefix along with a fixed length number (e.g., ABC0000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions.

       iv.   Confidentiality designations, if any, will be endorsed on the lower left corner of all TIFF images;

       v.   For replacement documents, append "-R" to the Bates number.

B.   Images will be delivered with an image load file in the Opticon (.OPT) file format.

C.   Images, native files, and text files should be stored and delivered in separate folders named "IMAGES," "TEXT" and "NATIVE." Folders should be segmented into directories not to exceed 5,000 files.

D.   A transmittal cover letter should accompany each production that includes the production volume name(s), bate(s) ranges, custodians and associated document count, total number of records included in the production(s), total number of image, text and native files as well as the encryption method/software (do not include password in transmittal letter). If one or more production numbers is skipped in a production, the producing Party will so note in a cover letter accompanying the production or in a privilege log.

9.   **SEARCHABLE TEXT**

A.   Searchable text of entire documents will be produced either as extracted text for

all documents that originate in electronic format, or, for any document from which text cannot be extracted, as text generated using Optical Character Recognition (OCR) technology. OCR text will be provided for all documents that originate from hard copy or paper format. For redacted documents, the full text of the redacted version of the document will be produced.

B.   Searchable text will be produced as a document-level multi-page ASCII text file with the text file named the same as the PRODBEG field, placed in a separate folder. The full path of the text file must be provided in the .DAT file for the TEXT field.

10.   NATIVE FILES

A.   Native file documents, emails and/or attachments may be included with the electronic production using the below criteria:

i.   Documents produced in native format shall be re-named to reflect the production number.

ii.   The full path of the native file must be provided in the .DAT file for the NATIVE FILE field;

iii.   The confidentiality designation under the Stipulated Protective Order to be entered in this action will be produced in the load file in the CONFIDENTIALITY field.

iv.   The producing Party will produce a placeholder (a single-page TIFF slip sheet indicating that the native item was produced). The placeholder will be branded with the production number in the lower right-hand corner, the original filename of the native file, and the phrase "PRODUCED IN NATIVE" branded in the center of the page. The producing Party will also brand any confidentiality or similar endorsements in the lower left-

hand corner of the placeholder.

B.   If documents produced in native format are printed for use in deposition, motion or hearing, the Party printing the document must label the front page of the file that is printed with the corresponding production number and, if applicable, the confidentiality designation assigned by the producing Party to that file under an applicable protective order to be entered in this action.

C.   Excel spreadsheets should be produced in native format with lock/protect features and password protection disabled.

11.   EMBEDDED OBJECTS

A.   The Parties may exclude embedded objects from the production, so long as the relevant portion of the embedded object is maintained in the document produced. A Party seeking the full production of an embedded object shall meet and discuss with the other Parties the relevance of the full embedded object and the burden of reviewing and producing the full embedded object.

B.   Following production of the files containing embedded objects, a receiving Party may make reasonable requests, with respect to specific embedded objects particularly identified in the requests, for production of these embedded objects as stand-alone files. The producing Party shall cooperate reasonably in responding to any such requests.

12.   STRUCTURED DATA

To the extent a response to discovery requires production of electronic information stored in a database, the Parties will meet and confer to discuss format of production including whether relevant information may be provided by querying the database and generating a report in a reasonably usable and exportable electronic file. A document reference sheet shall be provided

to describe the purpose of the database and the meaning of relevant tables and column headers contained therein.

13.   DE-DUPLICATION

A.   Documents shall be de-duplicated across custodians prior to production. The Parties agree to use a verifiable, de-duplication process to ensure that one copy of a document is produced when feasible. A producing Party shall identify all custodians who were in possession of a de-duplicated documents in the "ALL CUSTODIAN" and "ALL FOLDER PATH" fields, listed in **Exhibit A**.

B.   For the avoidance of doubt, a document is not considered to be a duplicate in the case where email headers or attachments differ in any regard or where the same document is both attached to an email and exists in a form that is separate from such email (e.g., as an attachment to another email, as a standalone document saved to some electronic media, etc.).

C.   For good cause shown, the receiving Party shall have the right to request all duplicates of a produced document.

D.   Attachments will include files sent via hyperlinks in the possession, custody or control of the producing Party. For example, files attached via the "Share link" option in M365 will be treated the same as if they were attached as a copy.

14.   EMAIL THREADS

A.   Email threads are email communications that contain prior or lesser-inclusive email communications that also may exist separately in the Party's electronic files. A most inclusive email thread is one that contains all of the prior or lesser-inclusive emails, including attachments, for that branch of the email thread. Email thread suppression may not eliminate (a) the ability of a requesting Party to identify every custodian who had a copy of a produced

document or email, or (b) remove from a production any unique branches and/or attachments contained within an email thread.

B.   Each Party may produce only the most inclusive email threads.

C.   Similarly, a Party may list the most inclusive email thread on any required privilege log. However, if the most inclusive email thread contains privileged portions and would otherwise be logged in its entirety as privileged, then the thread must be produced with privileged material redacted and the redacted portion logged.

D.   Should there be a unique attachment connected to a prior or lesser-inclusive email communication, that prior or lesser-inclusive communication with the attachment must be produced.

E.   Following production of the most-inclusive email threads, a receiving Party may make reasonable requests, with respect to most-inclusive email threads particularly identified in the requests, for production of individual lesser-inclusive emails. The producing Party shall cooperate reasonably in responding to any such requests.

15.   **ARCHIVE FILE TYPES**

Archive file types (e.g., .zip, .rar) shall be uncompressed for processing. Each file contained within an archive file that hits on a search term shall be analyzed for relevance. If the archive file is itself an attachment, that parent/child relationship shall also be preserved.

16.   **MICROSOFT "AUTO" FEATURE**

To the extent reasonably practicable and technologically possible for a producing Party's vendor, Microsoft Excel (.xls) and Microsoft PowerPoint (.ppt) documents should be analyzed for the "auto" features, where documents have an automatically updated date and time in the document, file names, file paths, or similar information that when processed would be inaccurate

16

for how the document was used in the ordinary course of business. If "auto date," "auto file name," "auto file path," or similar features are identified, the produced document shall be branded with the words "Auto Date," "Auto File Name," or "Auto File Path" formula used or similar words that describe the "auto" feature.

17.   **COLOR**

Documents or records containing color (for example, graphs, pictures, color marketing materials, and text messages) will be produced as color images for each such document or record, to the extent possible. This provision does not apply to hard copy documents or electronic records containing color logos, signatures, watermarks, or letterhead.

18.   **SYSTEM FILES**

Electronic file collection will be "De-NISTed," removing commercially available operating system and application files contained on the National Institute of Standards and Technology ("NIST") file list. Identification of NIST list matches will be through MD5 Hash values.

19. **TIME ZONE.**

When processing ESI, Coordinated Universal Time (UTC) should be selected as the time zone.

20.   **TEXT MESSAGES**

To the extent Producing Party determines that there is responsive information within text messages, and that such information is subject to production in accordance with the Federal Rules of Civil Procedure, the Parties will meet and confer to discuss the search parameters and format of production of text messages. The Parties recognize that there is a wide variety of capabilities available, and it is difficult to assert a standard into a protocol without information

as to each Party's capabilities.

21.   MOBILE APPLICATION DATA

To the extent Producing Party determines that there is responsive information within mobile application data, and that such information is subject to production in accordance with the Federal Rules of Civil Procedure, the Parties will meet and confer to discuss the search parameters and format of production of mobile application data. The Parties recognize that there is a wide variety of capabilities available, and it is difficult to assert a standard into a protocol without information as to each Party's capabilities.

22.   COLLABORATION SOFTWARE PROGRAMS

To the extent Producing Party determines that there is responsive information within collaboration software programs, and that such information is subject to production in accordance with the Federal Rules of Civil Procedure, the Parties will meet and confer to discuss the search parameters and format of production of collaboration program data such as Microsoft TEAMS, Google Chat, or Slack. The Parties recognize that there is a wide variety of capabilities available, and it is difficult to assert a standard into a protocol without information as to each Party's capabilities.

23.   PRIVILEGE, PRIVILEGE LOGS AND REDACTIONS

A.   The parties may withhold documents subject to a valid assertion of privilege from production, in whole or in part, by designating the documents privileged pursuant to a claim of attorney-client privilege, work product protection, or other applicable privilege or immunity. Within a reasonable time after the conclusion of document production, the producing party will produce a privilege log in computer searchable form setting out information sufficient to satisfy the requirements of Federal Rule of Civil Procedure 26(b)(5), identifying, at a minimum:

    i.   Bates number or other identifier;

    ii.   Name(s) of the Document author(s), to the extent available in the metadata;

    iii.   Name(s) of the Document recipient(s);

    iv.   The date the Document was created, sent, and received, to the extent available in the metadata;

    v.   The type or format of the Document (e.g. email, spreadsheet, PowerPoint, etc.);

    vi.   The Document custodian(s);

    vii.   The Document title or (for emails) subject; and

    viii.   The basis for the assertion of privilege, including a general description of the privileged information.

B.   The producing party shall indicate, on the privilege log or otherwise in a list delivered with the privilege log, which individuals listed on the log are attorneys, and any persons working at the direction of attorneys, including, but not limited to, paralegals and support staff.

C.   A single Document containing multiple email messages (i.e., in an email chain) may be logged as a single entry. A Document family (e.g., email and attachments) may be logged as a single entry so long as the log entry accurately describes both the email and its attachment(s).

D.   Communications seeking legal advice, discussing legal strategy, or discussing work-product and involving inside or outside counsel for the Parties related to this case need not be placed on a privilege log, unless such communications include third parties to whom the work product privilege does not apply.

19

E.	The Parties agree to furnish logs that comply with Fed. R. Civ. P. 26(b)(5) and any other legal requirements for all documents withheld or redacted on the basis of privilege, attorney work product, or similar doctrines. Privilege logs may be produced on a rolling basis or after all productions are complete, but prior to the close of discovery.

F.	Upon any party's challenge to a claim of privilege, or to challenge a failure to provide a complete privilege log, the parties shall promptly meet and confer to attempt to resolve the issue(s) prior to the challenging party raising any unresolved issue(s) with the Court.

G.	Nothing in this Order shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity. The Parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of documents and ESI.

## 24.	EFFECT OF PROTOCOL AND RESERVATION OF RIGHTS

A.	The Parties agree to be bound by this Order during the sharing of ESI. Nothing in this Protocol precludes any Party from challenging the admissibility, discoverability, production, or confidentiality of information produced under this Protocol or otherwise objecting to its production or use during the merits hearing or during any other hearing.

B.	No Party may seek relief from the Court concerning compliance with the Protocol unless it has first conferred with the other Parties.

C.	The Protocol may be amended by the written agreement of the Parties, without the approval of the Court.

D.	Nothing in this Protocol shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity.

E.   Nothing contained herein is intended to or shall serve to limit a Party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

SO STIPULATED AND AGREED.

/s/ Rachel Soffin
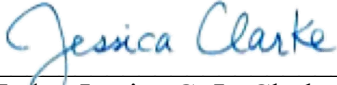Rachel Soffin
Counsel for Plaintiffs

Dated: June 3, 2024

/s/ Nilda M. Isidro
Nilda M. Isidro
Counsel for Defendants

Dated: June 3, 2024

So Ordered.

DATED: June 4, 2024

Jessica Clarke
_____
Judge Jessica G. L. Clarke
U.S. District Judge

EXHIBIT A

	Field	Definition	Applicable Doc Type
1	CUSTODIAN	Name of person or data source from where documents/files are produced. Where redundant names occur, individuals should be distinguished by an initial which is kept constant throughout productions (e.g., Smith, John A. and Smith, John B.).	All
2	PRODBEG	Beginning Bates number (production number)	All
3	PRODEND	Ending Bates number (production number)	All
4	BEGATT	First Bates number of family range (i.e. Bates number of the first page of the parent email)	All
5	ENDATT	Last Bates number of family range (i.e. Bates number of the last page of the last attachment)	All
6	PGCOUNT	Number of pages in the document	All
7	ATTACHCOUNT	Number of attachments to an email	All
8	FILENAME	Name of original file name of an E-Doc or attachment to an email	E-docs
9	DOCEXT	File extension of the document	All
10	MSGID	Value extracted from parent message during processing	Email
11	EMAILFROM	Sender	Email
12	EMAILTO	Recipient	Email
13	EMAILCC	Additional recipients	Email
14	EMAILBCC	Blind additional recipients	Email
15	EMAILSUBJECT	Subject line of email	Email
16	DATE-TIME SENT (mm/dd/yyyy hh:mm:ss)	Date and time sent	Email

	Field	Definition	Applicable Doc Type
17	DATE-TIME RCVD (mm/dd/yyyy hh:mm:ss)	Date and time received	Email
18	HASHVALUE	MD5 Hash Value	Email, Edocs
19	TITLE	Title provided by user within the document	Edocs
20	AUTHOR	Creator of a document	Edocs
21	DATECRTD (mm/dd/yyyy)	Creation date	Edocs
22	DATELASTMOD (mm/dd/yyyy)	Last modified date	Edocs
23	DOCTYPE	Descriptor of the type of document: "**E-document**" for electronic documents not attached to emails; "**Emails**" for all emails; "**E-attachments**" for files that are attachments to emails; and "**Paper**" for hard copy physical documents that have been scanned and converted to an electronic image	All
24	REDACTED	Descriptor for documents that have been redacted. "Yes" for redacted documents; "No" for unredacted documents.	All
25	PRODVOL	Name of media that data was produced on.	All
26	CONFIDENTIALITY	Indicates if the document has been designated as "Confidential" or "Highly Confidential" pursuant to any applicable Protective Order. "No" indicates those documents that are not so designated.	All
27	TEXTPATH	Full path for OCR or Extracted Text files on producing media	All

	Field	Definition	Applicable Doc Type
28	NATIVEFILELINK	Full path for documents provided in native format on producing media	Edocs
29	ALL CUSTODIAN	Name(s) of all custodian(s) that possessed the document; includes any custodian(s) whose duplicate file(s) was removed during processing.	Email
30	FOLDERPATH	File source path for all electronically collected documents and emails, which includes location, folder name and file extension.	Edocs
31	ALL FOLDERPATH	This field will include data for all custodians identified as duplicates. This field will be updated regularly to account for rolling productions.	
32	EMAIL IMPORTANCE	(Low, Normal or High)	Email
33	EMAIL SENSITIVITY	Normal, Personal, Private or Confidential	Email
34	REPLACEMENT	Flag Yes or No	All
35	TITLE	Title field value extracted from the native file metadata.	E-docs
36	CATEGORIES	Category value pulled from native file metadata	E-docs
37	SUBJECT	Subject field value extracted from native file metadata. Subject field is for e-docs only. Email subject field is for e-mail messages	E-docs
38	COMMENTS	Comments value pulled from the native file metadata	E-docs
39	KEYWORDS/TAGS	From document metadata	E-docs
40	HIDDENTEXT	Document has hidden text (Y/N)	All
41	SUSPECTOLE	Document contains embedded files. (Y/N)	All
42	HASCOMMENTS	Microsoft Word, Excel, or PowerPoint document contains comments	Microsoft E-docs

	Field	Definition	Applicable Doc Type
43	HASTRACKCHANGES	Microsoft Word or Excel document contains tracked changes.	Microsoft E-docs
44	APPLICATION NAME	Application value pulled from native file metadata.	E-docs
45	CAL START	Start date and time of calendar or appointment	E-mails, E-attachments and Electronic documents
46	CONVERSATION_INDEX	E-mail thread identification.	E-mail
47	CONVERSATION	Normalized subject of e-mails.	E-mail